

# IMPORTANT NOTICE FOR IRS CONTRACTORS



Access, Use or Operation of IRS Information Technology (IT) Systems by Contractors

**A New IRS Contract Clause Includes Consequences for Contractor Employees Who Violate IRS IT Security Policy On Using the Internet or E-mail.**

Contracting Officers at the IRS are including the contract clause in new and current IRS IT support services contracts. The clause will be included in the contracts when contractor employees will or have been authorized staff-like (unescorted) access to IRS owned or controlled facilities and information systems in performance of the contract. Contractors must include the clause in subcontracts that require staff-like access, comply with the clause requirements and assume responsibility for compliance by his/her employees. When an employee is removed for security violations, the contractor must also provide replacement personnel acceptable to the Contracting Officer's Technical Representative (COTR) within five days of official notification by the IRS. New hires or substitutions of personnel are subject to an acceptable IRS security screening, prior to being authorized staff-like access.

**Contractor Awareness of IRS IT Security Policy and Guidance.** Current and new IRS contractor employees authorized information systems and facilities access shall become aware of and comply with the IRS IT Security Policy and Guidance, Internal Revenue Manual (IRM) 25.10.1. A copy of the IRM may be requested from the Contracting Officer or Contracting Officer Technical Representative (COTR).

**Contractor Acknowledgement.** The contractor must acknowledge that the company and its employees assigned to the IRS IT contract understand that a contractor employee's unsanctioned, negligent, or willful violation of the laws, IRS system security rules, IRS security policies, standards, and procedures may result in the revocation of all access to IRS IT systems and facilities and immediate removal from IRS premises and the contract. For violations of Federal Statutes or State laws, the contractor employee may be arrested by Federal law enforcement agents and referred for criminal prosecution.

**Unauthorized Use of IRS Resources.** Some prohibited uses of the IRS computers are (1) accessing child pornography, bondage and bestiality, obscenity or other types of images that violate criminal law; (2) creating, downloading, viewing, storing, copying, or transmitting sexually explicit or sexually oriented materials such as adult pornography; (3) accessing personal e-mail accounts such as AOL or Hotmail through the IRS Internet firewall, hacker's information or tools, chat rooms (involving instant messaging) or gambling sites; (4) downloading, copying, and/or playing of computer video games. This is not an inclusive list. The IRS Employee Limited Personal Use Policy does not apply to contractor employees.



**Monitoring Notification.** The IRS monitors all users of its computers. Contractor employees do not have a right, nor should they have an expectation of privacy while using any IRS IT systems at any time, including accessing the Internet or using e-mail. Data maintained on Government office equipment may be subject to discovery and Freedom of Information Act requests. Any use of Government IT systems is made with the understanding that such use is generally not secure, is not private and is not anonymous.